On the Factorization of Trinomials over F3

Pierre Loidreau

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On the Factorization of Trinomials over $\mathbf{F}_3$

Pierre Loidreau

N° 3918

Avril 2000

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--3918--FR+ENG

On the Factorization of Trinomials over $\mathbf{F}_3$

Pierre Loidreau*

Thème 2 — Génie logiciel
et calcul symbolique
Projet CODES

Rapport de recherche n° 3918 — Avril 2000 — 18 pages

Abstract: We construct a table giving the parity of the number of factors in the factorization of trinomials over GF(3). The results depend on the value of the degrees of the monomials and their coefficients. We deduce results on the irreducibility of trinomials, on how to diminish the cost of irreducibility testing over GF(3) as well as on the primitivity of trinomials.

Key-words: Trinomials, cyclic codes, sequences, LFSR, stream ciphers

* Pierre.Loidreau@inria.fr

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Sur la factorisation des trinômes sur $\mathbf{F}_3$

Résumé : Nous construisons une table qui donne le nombre de facteurs modulo 2 dans la factorisation de trinômes sur GF(3). Le résultat dépend de la valeur des degrés des monômes et de leurs coefficients. Nous déduisons des résultats sur l'irréductibilité des trinômes, et sur comment diminuer le cou6t algorithmique du test d'irréductibilité sur GF(3) ainsi que du test de primitivité.

Mots-clés : Trinômes, Codes cycliques, séquences, LFSR, chiffrement à flots

Introduction

Trinomials are polynomials with three non-zero coefficients. It is well known that trinomials over Finite fields are of most interest in a number of applications. For instance they are the words of weight 3 in some cyclic codes [CTZ97] . Their properties are also strongly related to the characterization of almost perfect non-linear boolean functions [CCZ98] or with sequences that have the "trinomial property" (introduced by S. W. Golomb [Gol67]). Their use is also recognized in the field of cryptography since Canteaut and Filiol presented an attack on stream ciphers by identifying the factors of some trinomial [CF] following the ideas of Meier and Staffelbach [MS89].

Whereas the binary case has been particularly studied, people are becoming interested in problems over fields with an odd characteristic. In [CTZ97], Charpin, Tietäväinen and Zinoviev study the minimal distance of some cyclic codes on any prime non binary field and consider the special case GF(3). On the other hand Helleseth, Rong and Sandberg constructed several new infinite families of nonbinary APN mappings [HRS99]. These papers are both related with the properties of trinomials over GF(3).

In the paper we produce a table giving the parity of the number of factors in the factorization of trinomials over GF(3) depending on the degree of its monomials. This induces some natural applications like the study of the irreducibility of trinomials over GF(3). The paper is based on an application of Swan's results [Swa62] which link the value of the discriminant and the parity of the number of factors of a polynomial. This very paper also gives an explicit formula to calculate the discriminant of trinomials over any finite field. We first recall the general results linking the value of the discriminant and the parity of the number of factors. We then determine the value of the discriminant of trinomials over $\mathbf{F}_3$ by splitting the study into several cases depending on the value of the exponents and of the coefficients. Hence we exhibit a table providing the parity of the number of factors of trinomials depending on the degree of the monomials and the values of the coefficients. From this we also deduce cases where the trinomials cannot be irreducible and cases where the trinomials cannot be primitive.

1 Preliminaries

Discriminant of polynomials

Definition 1 *Let* $\mathbf{F}_{p^m}$ *be the finite field of characteristic* p *odd or even with* p^m *elements, let* $f(x) \in \mathbf{F}_{p^m}[x]$ *and* $\mathbf{F}_{p^{mt}}$ *be the splitting field of* f*. Then the discriminant of the polynomial* f *is the quantity* $D(f) \in \mathbf{F}_{p^{mt}}$ *such that*

$$D(f) = (-1)^{n(n-1)/2} \prod_{\alpha_i \neq \alpha_j} (\alpha_i - \alpha_j)$$

where the $(\alpha_i)_{i=1}^n \in \mathbf{F}_{p^{mt}}$ *are the roots of* f *counted with multiplicity.*

Hence we deduce the following properties

- Since $D(f)$ is a symmetric function of the roots of f, $D(f)$ belongs to the coefficient field of f, *i.e.*

$$D(f) \in \mathbf{F}_{p^m} \subset \mathbf{F}_{p^{mt}}$$

- $D(f) = 0 \iff f$ has multiple roots

Discriminant and factorization There exist a tight link between the value of the discriminant of a polynomial and the parity of the number of factors in its factorization. The general result has been proven by Swan in [Swa62]. By applying the theorem to polynomials over $\mathbf{F}_{p^m}$ where p is odd, we have

Theorem 1 *Let $\mathbf{F}_{p^m}$ be a finite field of odd characteristic, let $f(x) \in \mathbf{F}_{p^m}[x]$ be of degree n, let r be the number of irreducible factors of $f(x)$ over $\mathbf{F}_{p^m}$, then*

$$r \equiv n \bmod 2 \iff D(f) \text{ is a square in } \mathbf{F}_{p^m}$$

Discriminant of trinomials Given a polynomial over some field it is not possible in general to determine an explicit formula for its discriminant. However, in the case where the polynomial $f(x)$ is of the form

$$f(x) = x^n + ax^k + b$$

one has [Swa62]

Theorem 2 *Let $n > k > 0$, $d = GCD(n,k)$ and $n = n_1 d$, $k = k_1 d$, then*

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} \left[n^{n_1} b^{n_1 - k_1} - (-1)^{n_1} (n-k)^{n_1 - k_1} k^{k_1} a^{n_1} \right]^d$$

2 Discriminant of trinomials over $\mathbf{F}_3$

In the following of the paper, we deal with trinomials over the field with odd characteristic $\mathbf{F}_3$.

From **Theorem** 1, to study the parity of the number of factors of trinomials with coefficients in $\mathbf{F}_3$ one has to evaluate the discriminant of the trinomials over $\mathbf{F}_3$. In the case of trinomials we use the general formula given in **Theorem** 2.

Trinomials over $\mathbf{F}_3$ There are four monic trinomials with coefficients in the field $\mathbf{F}_3 = \{0, 1, -1\}$:

$$x^n + x^k + 1,\ x^n + x^k - 1,\ x^n - x^k + 1,\ x^n - x^k - 1$$

Evaluation of the discriminant Since from **Theorem** 2

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} \left[n^{n_1} b^{n_1-k_1} - (-1)^{n_1} (n-k)^{n_1-k_1} k^{k_1} a^{n_1} \right]^d$$

to calculate the discriminant taking values in $\mathbf{F}_3$, one must consider

1. the values of $a,\ b$ in $\mathbf{F}_3$, that is the type of the trinomial,
2. the values of n and k taken in the field $\mathbf{F}_3$, *i.e.* the integers n and k reduced modulo 3,
3. the value of $(-1)^{n(n-1)/2}$ depending on the value of n modulo 4,
4. the parity of d, the GCD of n and k. It depends on the parity of n and k, namely

$$d \equiv 0 \bmod 2 \iff n,\ k \equiv 0 \bmod 2$$

5. the parity of n_1 and k_1 where $n = dn_1$ and $k = dk_1$.

   To determine the parity of these parameters, we must introduce the binary valuation over integers

   Definition 2 *Let n be an integer and let us define the operator v_2 by*

$$\begin{cases} n = 2^{v_2(n)} n_2, \\ n_2 \text{ is odd} \end{cases}$$

   $v_2(n)$ is denoted binary valuation of n

   From this definition we deduce the following proposition about the parity of $n_1,\ k_1,\ n_1 - k_1$

   Proposition 1 *Let $n = n_1 d,\ k = k_1 d$ be two integers where $d = GCD(n,k)$ then*

   - n_1 *is even* $\iff v_2(n) > v_2(k)$,
   - k_1 *is even* $\iff v_2(n) < v_2(k)$,
   - $n_1 - k_1$ *is even* $\iff v_2(n) = v_2(k)$,

From the previous remarks, we have to separate the study of trinomial over $\mathbf{F}_3$ into several cases dealing not only with the value of the parameters $a,\ b,\ n,\ k$ taken in $\mathbf{F}_3$ but also with the parity of n and k and their binary valuation.

3 Degree equivalent to 0 mod 3

Since the degree n is such that $n \equiv 0 \bmod 3$, the term $n^{n_1} b^{n_1-k_1}$ in the expression of the discriminant vanishes. Hence

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} (-1)^{d-k} k^n a^n$$

since a and b are non zero elements in $\mathbf{F}_3$, the discriminant $D(x^n + ax^k + b)$ is equal to zero if and only if k is a multiple of 3, thus

Proposition 2 *If $n \equiv 0 \bmod 3$, then the trinomial $x^n + ax^k + b$ has multiple roots if and only if $k \equiv 0 \bmod 3$.*

In every other case, we have to split the trinomials regarding the values of n modulo 12 and k modulo 6. In the following of the section, we suppose that k is non zero in $\mathbf{F}_3$

Theorem 3 *If $n \equiv 0 \bmod 3$ and $k \neq 0 \bmod 3$ then*

- $D(x^n + x^k + 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 0 \bmod 12, \quad k \equiv 1, 2 \bmod 3 \\ n &\equiv 3 \bmod 12, \quad k \equiv 4, 5 \bmod 6 \\ n &\equiv 9 \bmod 12, \quad k \equiv 1, 2 \bmod 6 \end{aligned}$$

- $D(x^n + x^k - 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 0 \bmod 12, \quad k \equiv 1, 5 \bmod 6 \\ n &\equiv 3 \bmod 12, \quad k \equiv 2 \bmod 3 \\ n &\equiv 6 \bmod 12, \quad k \equiv 2, 4 \bmod 6 \\ n &\equiv 9 \bmod 12, \quad k \equiv 1 \bmod 3 \end{aligned}$$

- $D(x^n - x^k + 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 0 \bmod 12, \quad k \equiv 1, 2 \bmod 3 \\ n &\equiv 3 \bmod 12, \quad k \equiv 1, 2 \bmod 3 \\ n &\equiv 9 \bmod 12, \quad k \equiv 4, 5 \bmod 6 \end{aligned}$$

- $D(x^n - x^k - 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 0 \bmod 12, \quad k \equiv 1, 5 \bmod 6 \\ n &\equiv 3 \bmod 12, \quad k \equiv 1 \bmod 3 \\ n &\equiv 6 \bmod 12, \quad k \equiv 2, 4 \bmod 6 \\ n &\equiv 9 \bmod 12, \quad k \equiv 2 \bmod 3 \end{aligned}$$

Proof We first study the trinomial $T_1 = x^n + x^k + 1$.
We separate it in two cases

1. if n is even that is $n \equiv 0 \bmod 12$ or $n \equiv 6 \bmod 12$.

   Since k is non-zero in $\mathbf{F}_3$, then $k^n \equiv 1 \bmod 3$ whatever k be.

   Since d is even is even if and only if k is even, $d - k$ is even whatever k be. Hence

   $$D(T_1) = (-1)^{n(n-1)/2}$$

   it follows that $D(T_1)$ is equal to 1 if and only if $n \equiv 0 \bmod 12$.

2. if n is odd, then $k^n \equiv k \bmod 3$ and the GCD d of n and k is also odd, thus

   $$D(T_1) = (-1)^{n(n-1)/2} \cdot (-1)^{k+1} \cdot k$$

   and since k is non-zero in $\mathbf{F}_3$

   $$D(T_1) = 1 \Longleftrightarrow \begin{cases} n \equiv 3 \bmod 12, & k \equiv 4, 5 \bmod 6 \\ n \equiv 9 \bmod 12, & k \equiv 1, 2 \bmod 6 \end{cases}$$

Since $D(x^n + ax^k + b) = b^{k-1} a^n D(T_1)$, we deduce the result for the other trinomials from $D(T_1)$. ■

4 Degree equivalent to $1 \bmod 3$

In that case, there is no simplification of the expression of the discriminant. It has to be studied for every possible trinomial. Namely the discriminant becomes

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} \left[b^{n_1 - k_1} - (-1)^{n_1} (1-k)^{n_1 - k_1} k^{k_1} a^{n_1} \right]^d$$

where d is the GCD of n and k and $n = n_1 d$, $k = k_1 d$. The value of the discriminant depends thus not only on the value of n and k modulo 3 but also on the parity of n_1, k_1, d, that is on the valuation v_2 of n and k.

4.1 Trinomial $x^n + x^k + 1$

For the trinomial $x^n + x^k + 1$, the discriminant is

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2} \left[1 - (-1)^{n_1} (1-k)^{n_1 - k_1} k^{k_1} \right]^d$$

Theorem 4 *If* $n \equiv 1 \bmod 3$, *then*

- $x^n + x^k + 1$ *has multiple roots if and only if* $D(x^n + x^k + 1) = 0$ *that is if and only if*

  $$k \equiv 2 \bmod 3$$

- *in every other case,* $D(x^n + x^k + 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 1 \bmod 12, \quad & k &\equiv 0, 1 \bmod 3 \\ n &\equiv 4 \bmod 12, \quad & k &\equiv 0, 1 \bmod 3 \end{aligned}$$

Proof We separate it in two cases

1. case $k \equiv 2 \bmod 3$

   We have

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2} \left[1 - (-1)^{n_1}(-1)^{n_1 - k_1}(-1)^{k_1}\right]^d = 0$$

   hence the trinomial $x^n + x^k + 1$ has multiple roots if and only if $k \equiv 2 \bmod 3$,

2. case $k \equiv 0, 1 \bmod 3$

   Either k or $1 - k$ is equal to 0 in $\mathbf{F}_3$ thus the term $(-1)^{n_1}(1-k)^{n_1-k_1}k^{k_1}$ in the expression of the discriminant vanishes and

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2}$$

   hence the discriminant is never equal to 0 and

$$D(x^n + x^k + 1) = 1 \Longleftrightarrow n \equiv 1, 4 \bmod 12$$

■

4.2 Trinomial $x^n + x^k - 1$

For the trinomial $x^n + x^k - 1$, the discriminant is

$$D(x^n + x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}\left[(-1)^{n_1-k_1} - (-1)^{n_1}(1-k)^{n_1-k_1}k^{k_1}\right]^d$$

Theorem 5 *If* $n \equiv 1 \bmod 3$, *then*

- $x^n + x^k - 1$ *has multiple roots if and only if* $D(x^n + x^k - 1) = 0$ *that is if and only if*

$$k \equiv 2 \bmod 3 \text{ and } v_2(k) = v_2(n)$$

  where v_2 *is the binary valuation.*

- *in every other case,* $D(x^n + x^k - 1) = 1$ *if and only if*

$$\begin{aligned} n &\equiv 1 \bmod 12, \quad & k &\equiv 0, 1 \bmod 3 \\ n &\equiv 4 \bmod 12, \quad & & & k &\equiv 5 \bmod 6 \\ n &\equiv 7 \bmod 12, \quad & & & k &\equiv 2 \bmod 6 \\ n &\equiv 10 \bmod 12, \quad & k &\equiv 0, 1 \bmod 3, \quad & k &\equiv 2 \bmod 6 \end{aligned}$$

Proof We separate it in two cases

1. case $k \equiv 0, 1 \bmod 3$

   Either k or $1-k$ is equal to 0 in $\mathbf{F}_3$ thus the term $(-1)^{n_1}(1-k)^{n_1-k_1}k^{k_1}$ in the expression of the discriminant vanishes and

   $$D(x^n + x^k - 1) = (-1)^{n(n-1)/2}(-1)^{n-1}$$

   hence the discriminant is never equal to 0 and

   $$D(x^n + x^k - 1) = 1 \Longleftrightarrow n \equiv 1, 10 \bmod 12$$

2. case $k \equiv 2 \bmod 3$

   We have

   $$D(x^n + x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}\left[(-1)^{n_1-k_1} - 1\right]^d$$

   thus $D(x^n + x^k - 1) = 0$ if and only if $n_1 - k_1$ is even that is from **Proposition** 1 if and only if $v_2(k) = v_2(n)$

   If $v_2(k) \neq v_2(n)$ then $(-1)^{n_1-k_1} - 1 = 1$ in $\mathbf{F}_3$ and

   $$D(x^n + x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}$$

   and in that case

   $$D(x^n + x^k - 1) = 1 \iff \begin{cases} n \equiv 4 \bmod 12, & k \equiv 5 \bmod 6 \\ n \equiv 7 \bmod 12, & k \equiv 2 \bmod 6 \\ n \equiv 10 \bmod 12, & k \equiv 2 \bmod 6 \end{cases}$$

■

4.3 Trinomial $x^n - x^k + 1$

For the trinomial $x^n - x^k + 1$, the discriminant is

$$D(x^n - x^k + 1) = (-1)^{n(n-1)/2}\left[1 - (1-k)^{n_1-k_1}k^{k_1}\right]^d$$

Theorem 6 *If* $n \equiv 1 \bmod 3$ *then*

- $x^n - x^k + 1$ *has multiple roots if and only if* $D(x^n - x^k + 1) = 0$ *that is if and only if*

  $$k \equiv 2 \bmod 3 \text{ and } v_2(k) < v_2(n)$$

  where v_2 *is the binary valuation*

- *in every other case,* $D(x^n - x^k + 1) = 1$ *if and only if*

  $$\begin{array}{lll} n \equiv 1 \bmod 12, & k \equiv 0, 1 \bmod 3 & \\ n \equiv 4 \bmod 12, & k \equiv 0, 1 \bmod 3, & k \equiv 2 \bmod 6 \\ n \equiv 7 \bmod 12, & & k \equiv 5 \bmod 6 \end{array}$$

Proof We separate the proof in two cases

1. case $k \equiv 2 \bmod 3$

   We have

   $$D(x^n - x^k + 1) = (-1)^{n(n-1)/2} \left[1 - (-1)^{n_1}\right]^d$$

   the discriminant is null if and only if n_1 is even, which from **Proposition** 1 is equivalent to $v_2(k) < v_2(n)$

   Whenever $v_2(k) \geq v_2(n)$, we have

   $$D(x^n - x^k + 1) = (-1)^{n(n-1)/2}(-1)^d$$

   since d is even if and only if n and k are even, if $k \equiv 2 \bmod 3$ then we have

   $$D(x^n - x^k + 1) = 1 \iff \begin{cases} n \equiv 4 \bmod 12, & k \equiv 2 \bmod 6 \\ n \equiv 7 \bmod 12, & k \equiv 5 \bmod 6 \end{cases}$$

2. case $k \equiv 0, 1 \bmod 3$

   Either k or $1 - k$ is equal to 0 in $\mathbf{F}_3$ thus he term $(1-k)^{n_1 - k_1} k^{k_1}$ in the expression of the discriminant vanishes and

   $$D(x^n - x^k + 1) = (-1)^{n(n-1)/2}$$

   hence the discriminant is never equal to 0 and

   $$D(x^n - x^k + 1) = 1 \Longleftrightarrow n \equiv 1, 4 \bmod 12$$

4.4 Trinomial $x^n - x^k - 1$

For the trinomial $x^n - x^k - 1$ the discriminant is

$$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1} \left[(-1)^{n_1 - k_1} - (1-k)^{n_1 - k_1} k^{k_1}\right]^d$$

Theorem 7 *If $n \equiv 1 \bmod 3$ then*

- *$x^n - x^k - 1$ has multiple roots if and only if $D(x^n - x^k - 1) = 0$ that is if and only if*

  $$k \equiv 2 \bmod 3 \text{ and } v_2(k) > v_2(n)$$

  where v_2 is the binary valuation

- *in every other case, $D(x^n - x^k - 1) = 1$ if and only if*

  $$\begin{array}{lll} n \equiv 1 \bmod 12, & k \equiv 0, 1 \bmod 3 & \\ n \equiv 4 \bmod 12, & & k \equiv 5 \bmod 6 \\ n \equiv 7 \bmod 12, & & k \equiv 5 \bmod 6 \\ n \equiv 10 \bmod 12, & k \equiv 0, 1 \bmod 3, & k \equiv 2 \bmod 6 \end{array}$$

Proof We separate the proof into two cases

1. case $k \equiv 2 \bmod 3$

   We have

   $$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^k \left[(-1)^{n_1-k_1} - (-1)^{n_1}\right]^d$$

   the discriminant is null if and only if k_1 is even, which from **Proposition** 1 is equivalent to $v_2(k) > v_2(k)$

   Whenever $v_2(k) \leq v_2(n)$, we have

   $$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}(-1)^n \left[(-1)^{k_1} - 1\right]^d$$

   since in that case k_1 is odd, we have $\left[(-1)^{k_1} - 1\right]^d = (-2)^d = 1^d$, thus

   $$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}(-1)^n$$

   and

   $$D(x^n - x^k - 1) = 1 \iff \begin{cases} n \equiv 4 \bmod 12, & k \equiv 5 \bmod 6 \\ n \equiv 7 \bmod 12, & k \equiv 5 \bmod 6 \\ n \equiv 10 \bmod 12, & k \equiv 2 \bmod 6 \end{cases}$$

2. case $k \equiv 0, 1 \bmod 3$

   Either k or $1 - k$ is equal to 0 in $\mathbf{F}_3$ thus term $(1-k)^{n_1-k_1}k^{k_1}$ in the expression of the discriminant vanishes and

   $$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^{k-1}(-1)^{n-k} = (-1)^{n(n-1)/2}(-1)^{n-1}$$

   the discriminant is thus never equal to 0 and depends only on the value of n modulo 3. Hence

   $$D(x^n - x^k - 1) = 1 \iff \begin{cases} n \equiv 1 \bmod 12, & k \equiv 0, 1 \bmod 3 \\ n \equiv 10 \bmod 12, & k \equiv 0, 1 \bmod 3 \end{cases}$$

5 Degree equivalent to 2 mod 3

In that case, we replace the value of n in the discriminant by the value -1 in $\mathbf{F}_3$ thus the expression of the discriminant is

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2}b^{k-1}(-1)^n \left[b^{n_1-k_1} - (-1)^{n_1-k_1}(1+k)^{n_1-k_1}k^{k_1}a^{n_1}\right]^d$$

where d is the GCD of n and k and $n = n_1 d$, $k = k_1 d$. The value of the discriminant depends thus not only on the value of n and k modulo 3 but also on the parity of n_1, k_1, d, that is on the valuation v_2 of n and k.

In this section the proofs of the theorems which have exactly the same form as in the previous section are skipped.

5.1 Trinomial $x^n + x^k + 1$

For the trinomial $x^n + x^k + 1$ the discriminant is

$$D(x^n + x^k + 1) = (-1)^{n(n-1)/2}(-1)^n \left[1 - (-1)^{n_1 - k_1}(1+k)^{n_1 - k_1} k^{k_1}\right]^d$$

Theorem 8 *If $n \equiv 2 \bmod 3$, then*

- *$x^n + x^k + 1$ has multiple roots if and only if $D(x^n + x^k + 1) = 0$ that is if and only if*

$$k \equiv 1 \bmod 3$$

- *in every other case, $D(x^n + x^k + 1) = 1$ if and only if*

$$\begin{aligned} n &\equiv 8 \bmod 12, \quad k \equiv 0, 2 \bmod 3 \\ n &\equiv 11 \bmod 12, \quad k \equiv 0, 2 \bmod 3 \end{aligned}$$

5.2 Trinomial $x^n + x^k - 1$

For the trinomial $x^n + x^k - 1$ the discriminant is

$$D(x^n + x^k - 1) = (-1)^{n(n-1)/2+1} \left[1 - (1+k)^{n_1 - k_1} k^{k_1}\right]^d$$

Theorem 9 *If $n \equiv 2 \bmod 3$, then*

- *$x^n + x^k - 1$ has multiple roots if and only if $D(x^n + x^k - 1) = 0$ that is if and only if*

$$k \equiv 1 \bmod 3 \text{ and } v_2(k) = v_2(n)$$

  where v_2 is the binary valuation.

- *in every other case, $D(x^n + x^k - 1) = 1$ if and only if*

$$\begin{aligned} n &\equiv 2 \bmod 12, \quad k \equiv 0, 2 \bmod 3, \quad k \equiv 4 \bmod 6 \\ n &\equiv 5 \bmod 12, \quad k \equiv 4 \bmod 6 \\ n &\equiv 8 \bmod 12, \quad k \equiv 1 \bmod 6 \\ n &\equiv 11 \bmod 12, \quad k \equiv 0, 2 \bmod 3 \end{aligned}$$

5.3 Trinomial $x^n - x^k + 1$

For the trinomial $x^n - x^k + 1$ the discriminant is

$$D(x^n - x^k + 1) = (-1)^{n(n-1)/2}(-1)^n \left[1 - (-1)^{k_1}(1+k)^{n_1-k_1}k^{k_1}\right]^d$$

Theorem 10 *If* $n \equiv 2 \bmod 3$, *then*

- $x^n - x^k + 1$ *has multiple roots if and only if* $D(x^n - x^k + 1) = 0$ *that is if and only if*

  $$k \equiv 1 \bmod 3 \text{ and } v_2(k) < v_2(n)$$

  where v_2 *is the binary valuation*

- *in every other case,* $D(x^n - x^k + 1) = 1$ *if and only if*

  $$\begin{array}{lll} n \equiv 5 \bmod 12, & k \equiv 1 \bmod 3 & \\ n \equiv 8 \bmod 12, & k \equiv 0,2 \bmod 3, & k \equiv 4 \bmod 6 \\ n \equiv 11 \bmod 12, & k \equiv 0,2 \bmod 3 & \end{array}$$

5.4 Trinomial $x^n - x^k - 1$

For the trinomial $x^n - x^k - 1$ the discriminant is

$$D(x^n - x^k - 1) = (-1)^{n(n-1)/2}(-1)^{n+k-1} \left[(-1)^{n_1-k_1} - (-1)^{k_1}(1+k)^{n_1-k_1}k^{k_1}\right]^d$$

Theorem 11 *If* $n \equiv 2 \bmod 3$, *then*

- $x^n - x^k - 1$ *has multiple roots if and only if* $D(x^n - x^k - 1) = 0$ *that is if and only if*

  $$k \equiv 1 \bmod 3 \text{ and } v_2(k) > v_2(n)$$

  where v_2 *is the binary valuation*

- *in every other case,* $D(x^n - x^k - 1) = 1$ *if and only if*

  $$\begin{array}{lll} n \equiv 2 \bmod 12, & k \equiv 0,2 \bmod 3, & k \equiv 4 \bmod 6 \\ n \equiv 5 \bmod 12, & & k \equiv 1 \bmod 6 \\ n \equiv 8 \bmod 12, & & k \equiv 1 \bmod 6 \\ n \equiv 11 \bmod 12, & k \equiv 0,2 \bmod 3 & \end{array}$$

6 Irreducibility testing

The results in the previous section can be used to obtain a table giving values of n and k for which one can find irreducible trinomials over $\mathbf{F}_3$.

Parity of the number of factors In the field $\mathbf{F}_3 = \{0,\ 1,\ -1\}$, the only non zero value which is a square is 1 thus by applying **Theorem** 1 to the polynomials over $\mathbf{F}_3$ we obtain

Corollary 1 *let $f(x) \in \mathbf{F}_3[x]$ be of degree n with no multiple roots* i.e. *$D(f) \neq 0$, let r be the number of irreducible factors of $f(x)$ over $\mathbf{F}_3$, then*

$$r \equiv n \ mod\ 2 \iff D(f) = 1$$

For every trinomial $x^n + ax^k + b$ and for every value of n, we build the following **Table 1**. This table gives the values of k for which the number of factors in the factorization of $x^n + ax^k + b$ over $\mathbf{F}_3$ is odd.

Irreducibility testing Since an irreducible polynomial is divided only by itself, the number of factors in its factorisation is odd. Hence the parameters of trinomials that are candidate to irreducibility have to be found in the table.

Irreducibility testing can thus be simplified. Suppose we want to test the irreducibility of a trinomial $x^n + ax^k + b$ over $\mathbf{F}_3$ such that $D(x^n + ax^k + b)$ is non-zero. We proceed the following way

1. if the entry k corresponding to the polynomial $x^n + ax^k + b$ is not in the table then $x^n + ax^k + b$ is not irreducible.
2. if the entry k is in the table then apply one of the known polynomial-time algorithms checking the irreducibility of a polynomial such as the Shoup algorithms [Sho90]

Remark

- 1 is root of the trinomial $x^n + x^k + 1$ in $\mathbf{F}_3$ whatever k and n be.
- **Table 1** shows that there are values of n for which it is not possible to find any irreducible trinomial,

7 Primitivity of trinomials

From the previous results we can deduce conditions on the parity of the exponent n for which a trinomial over $\mathbf{F}_3$ is primitive. In the section we do not consider the trinomial $x^n + x^k + 1$ which has a trivial root over $\mathbf{F}_3$ and is never primitive.

Table 1: Values of k for which the trinomials over $\mathbf{F}_3$have an odd number of factors

n	$x^n + x^k + 1$	$x^n + x^k - 1$
0 mod 12	no value for k	$k \equiv 2, 4 \bmod 6$
3 mod 12	$k \equiv 4, 5 \bmod 6$	$k \equiv 2 \bmod 3$
6 mod 12	$k \equiv 1, 2 \bmod 3$	$k \equiv 1, 5 \bmod 6$
9 mod 12	$k \equiv 1, 2 \bmod 6$	$k \equiv 1 \bmod 3$
1 mod 12	$k \equiv 0, 1 \bmod 3$	$k \equiv 0, 1 \bmod 3$
4 mod 12	no value for k	$k \equiv 0, 1 \bmod 3$, $k \equiv 2 \bmod 6,\ v_2(k) \neq v_2(n)$
7 mod 12	no value for k	$k \equiv 2 \bmod 6$
10 mod 12	$k \equiv 0, 1 \bmod 3$	$k \equiv 5 \bmod 6$
2 mod 12	$k \equiv 0, 2 \bmod 3$	$k \equiv 1 \bmod 6$
5 mod 12	no value for k	$k \equiv 4 \bmod 6$
8 mod 12	no value for k	$k \equiv 0, 2 \bmod 3$, $k \equiv 4 \bmod 6,\ v_2(k) \neq v_2(n)$
11 mod 12	$k \equiv 0, 2 \bmod 3$	$k \equiv 0, 2 \bmod 3$,
n	$x^n - x^k + 1$	$x^n - x^k - 1$
0 mod 12	no value for k	$k \equiv 2, 4 \bmod 6$
3 mod 12	$k \equiv 1, 2 \bmod 3$	$k \equiv 1 \bmod 3$
6 mod 12	$k \equiv 1, 2 \bmod 3$	$k \equiv 1, 5 \bmod 6$
9 mod 12	$k \equiv 4, 5 \bmod 6$	$k \equiv 2 \bmod 3$
1 mod 12	$k \equiv 0, 1 \bmod 3$	$k \equiv 0, 1 \bmod 3$
4 mod 12	no value for k	$k \equiv 0, 1 \bmod 3$, $k \equiv 2 \bmod 6,\ v_2(k) \leq v_2(n)$
7 mod 12	$k \equiv 5 \bmod 6$	$k \equiv 5 \bmod 6$
10 mod 12	$k \equiv 0, 1 \bmod 3$, $k \equiv 2 \bmod 6,\ v_2(k) \geq v_2(n)$	$k \equiv 5 \bmod 6$
2 mod 12	$k \equiv 0, 2 \bmod 3$, $k \equiv 4 \bmod 6$	$k \equiv 1 \bmod 6$
5 mod 12	$k \equiv 1 \bmod 3$	$k \equiv 1 \bmod 6$
8 mod 12	no value for k	$k \equiv 0, 2 \bmod 3$, $k \equiv 4 \bmod 6,\ v_2(k) \leq v_2(n)$
11 mod 12	$k \equiv 0, 2 \bmod 3$	$k \equiv 0, 2 \bmod 3$

General result The general result about the primitivity of a polynomial is the following [BGL94].

Theorem 12 *Let $f(x) = \sum_{i=0}^{n} f_i x^i$ be a polynomial with coefficients in the field $\mathbf{F}_q$ and let $F(x) = \sum_{i=0}^{n} f_i x^{2^i-1}$, then $f(x)$ is primitive over $\mathbf{F}_q$ if and only if $F(x)$ is irreducible over $\mathbf{F}_q$.*

Trinomials over $\mathbf{F}_3$ In the particular case of trinomials over $\mathbf{F}_3$ we have

Corollary 2 *The trinomial $x^n + ax^k + b$ over $\mathbf{F}_3$ is primitive if and only if the trinomial $x^{3^n-1} + ax^{3^k-1} + b$ is irreducible*

hence we deduce the following proposition

Proposition 3 *We have*

- *If $x^n + x^k - 1$ is primitive over $\mathbf{F}_3$ then n is even,*
- *if $x^n - x^k - 1$ is primitive over $\mathbf{F}_3$ then n is even,*
- *if $x^n - x^k + 1$ is primitive over $\mathbf{F}_3$ then n is odd.*

Proof For the proof, one has to consider the trinomials $x^{3^n-1} + ax^{3^k-1} + b$, then look in the table if there are possible irreducible trinomials over $\mathbf{F}_3$ for the parameter $3^n - 1$ and $3^k - 1$ and then apply **Corollary** 2

For all integer k, $3^k \equiv 3 \bmod 6$ and for all integer n,

$$3^n \equiv 3 \bmod 12 \iff n \text{ odd}$$

hence one has to consider the parity of n.

1. if n is odd then $3^n - 1 \equiv 2 \bmod 12$.

   The value $3^k - 1 \equiv 2 \bmod 6$ appears in **Table 1** only for the trinomial

   $$x^{3^n-1} - x^{3^k-1} + 1$$

   thus if n is odd, the trinomials $x^{3^n-1} + x^{3^k-1} - 1$ and $x^{3^n-1} - x^{3^k-1} - 1$ have either an even number of factor or a root over $\mathbf{F}_3$.

2. if n is even then $3^n - 1 \equiv 8 \bmod 12$.

   The value $3^k - 1 \equiv 2 \bmod 6$ appears in **Table 1** only for the trinomials

   $$x^{3^n-1} + x^{3^k-1} - 1,\ x^{3^n-1} - x^{3^k-1} - 1$$

   hence if n is even, the trinomial $x^{3^n-1} - x^{3^k-1} + 1$ has an even number of factors or a root over $\mathbf{F}_3$

■

References

[Ber84] E. R. Berlekamp. *Algebraic Coding Theory.* Aegean Press Park, revised edition, 1984.

[BGL94] Ian F. Blake, Shuhong Gao, and Robert Lambert. Constructive Problems for Irreducible Polynomials over Finite Fields. In *Third Canadian Workshop on Information theory and Applications*, pages 1–23, 1994.

[CCZ98] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, 15:125–156 (1998).

[CF] A. Canteaut and E. Filiol, Ciphertext Only Reconstruction of Stream Ciphers based on Combination Generators, submitted.

[CTZ99] P. Charpin, A. Tietäväinen, and V. Zinoviev. On the Minimum Distance of Non-binary Cyclic Codes. *Designs, Codes and Cryptography*, to appear.

[CTZ97] P. Charpin, A. Tietäväinen, and V. Zinoviev. On binary cyclic codes whose minimum distance is 3, *Problems of Information Transmission*, 33(3) (1997).

[GG99] Solomon W. Golomb and Guang Gong. Peridodic binary sequences with the "Trinomial Property". *IEEE Transactions on Information Theory*, 45(4):1276–1279, may 1999.

[Gol67] Solomon W. Golomb. *Shift Register Sequences.* Holden-Day, 1967.

[GZ68] Richard M. Goldstein and Neal Zierler. On Trinomial Recurrences. *IEEE Transactions on Information Theory*, 14(1):150–151, January 1968.

[HRS99] T. Helleseth, C. Rong and D. Sandberg, New families of almost perfect nonlinear power mappings, *IEEE transactions on Information Theory*, 45(2):475–495, March 1999.

[LN97] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, 2nd edition, 1997.

[Men93] Alfred J. Menezes. *Applications of Finite Fields.* Kluwer Academic Publishers, 1993.

[MS89] W. Meier and O. Staffelbach, Fast correlation attack on certain stream ciphers, *Jounal of Cryptology*, 1989, pp. 159-176.

[Mun98] Akihiro Munemasa. Orthogonal Arrays, Primitive Trinomials and Shift-Register Sequences. *Finite Fields and applications*, 4:252–260, 1998.

[Sho90] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54:435–447, 1990.

[Swa62] Richard G. Swan. Factorization of Polynomials over Finite Fields. *Pacific Journal of Mathematics*, 12(2):1099–1106, 1962.

[Vis97] Uzi Vishne. Factorization of Trinomials over Galois Fields of characteristic 2. *Finite Fields and applications*, 3:370–377, 1997.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399